

SECRET 40622450

160

MERCHANT

102

PRIVATE
DATABASE
 $m_i, i=1, \dots, N$

110

PUBLIC
DATABASE
 $(c_{1i}, c_{2i}, desc_i, tag_i)$
 $c_{1i} = (\gamma^T k_i, g^T) = E_{\{y\}}(k_i)$
 $c_{2i} = E_{\{k_{23}\}}(m_i)$

112

PAYMENT
SERVER

114

COMMUNICATION CHANNEL(S)

104

120

NETWORK

CUSTOMER

106

122

USER
DEVICE

FIG. 1

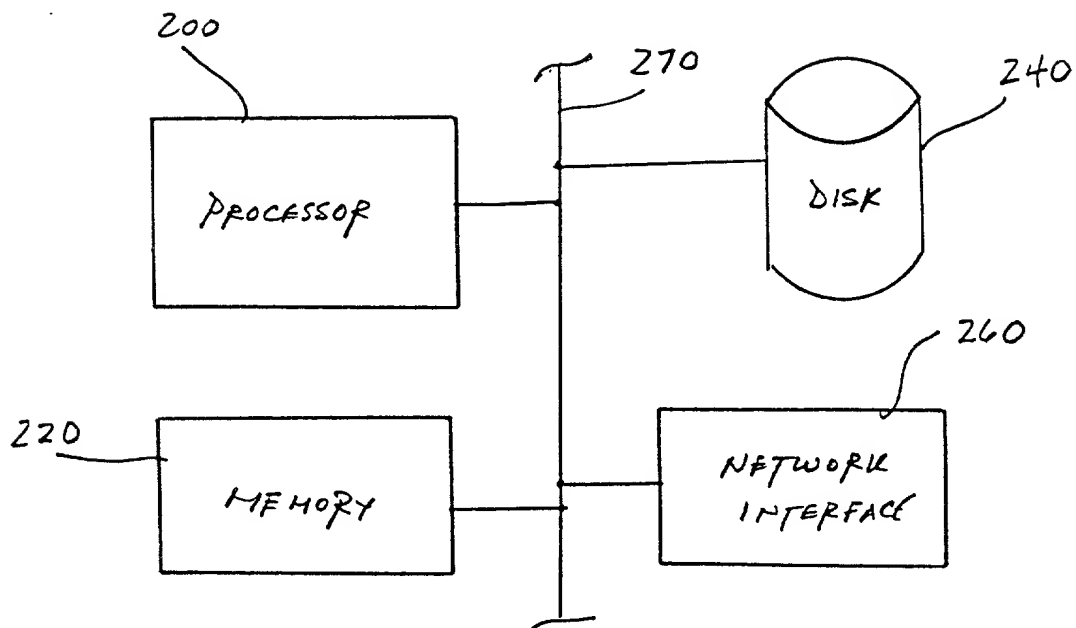


FIG. 2

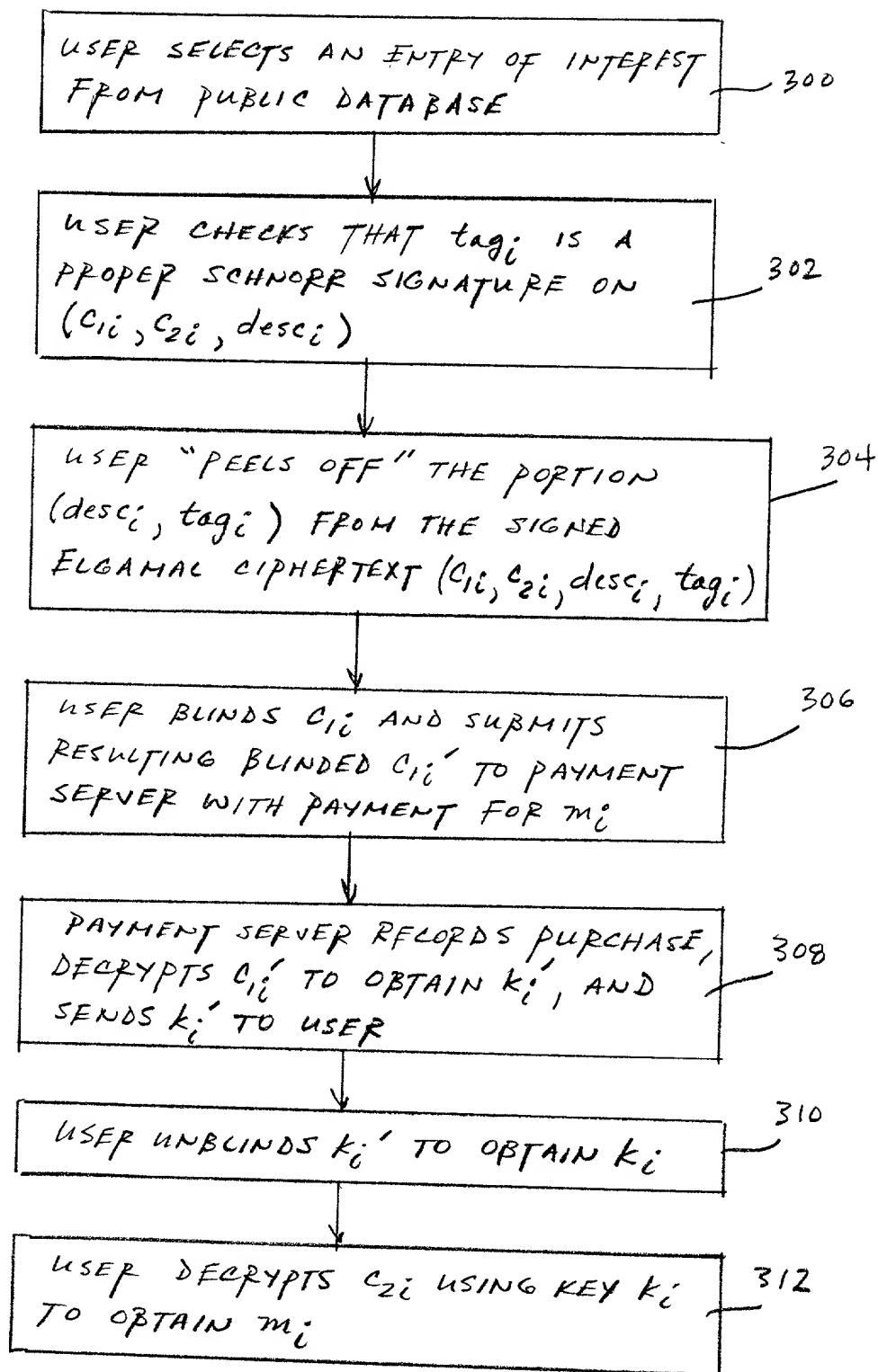


FIG. 3